FILED
2015 Feb-06 AM 10:07
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
MIDDLE DIVISION

PATRICIA MCNUTT and SCOTT HULSEY,	)	
	)	**CLASS ACTION COMPLAINT**
Plaintiffs,	)	
	)	
v.	)	**JURY TRIAL DEMANDED**
	)	
COMMUNITY HEALTH SYSTEMS, INC. and COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION,	)	**Case No. _____**
	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiffs, Patricia McNutt and Scott Hulsey, on behalf of themselves and all others similarly situated, for their Complaint against Defendants Community Health Systems, Inc. and Community Health Systems Professional Services Corporation (collectively referred to in the singular as "Community Health") allege as follows:

NATURE OF THE CASE

1. Plaintiffs bring this class action lawsuit against Community Health for its failure to protect its patients' personal and confidential sensitive information-including their protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), Social Security numbers, full

names, addresses, birthdates, telephone numbers and, possibly including, patient credit card, medical or clinical information (collectively, "Sensitive Information").

2. Community Health is one of the largest hospital organizations in the country, with over 206 facilities in 29 states.

3. As a health care provider, Community Health is required to protect its patients' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA.

4. In addition to its implied statutory obligation, Community Health expressly promises-through its privacy policies and patient agreements-to safeguard and protect the confidentiality of its patients' Sensitive Information in accordance with HIPAA regulations and industry standards.

5. As a result of Defendants' failure to implement and follow basic security procedures, Community Health's computer network was breached and approximately 4.5 million of its patients', including Plaintiffs, Sensitive Information is now in the hands of thieves. Plaintiffs now face a substantial increased risk of identity theft, if not actual identity theft. Consequently, Defendants' patients and former patients will have to spend significant time and money to protect themselves.

6. Additionally, as a result of Defendants' failure to follow contractually-agreed upon, federally-prescribed, industry standard security

procedures, Plaintiffs received only a diminished value of the services they paid Defendants to provide. Plaintiffs contracted for services that included a guarantee by Defendants to safeguard their personal information and, instead, Plaintiffs received services devoid of these very important protections.

PARTIES

7. Plaintiff Patricia McNutt, individually and as class representative, is a resident of DeKalb County, Alabama. McNutt received medical treatment at Gadsden Regional Medical Center in Etowah County, Alabama at all times material to this Complaint.

8. Plaintiff Scott Hulsey, individually and as class representative, is a resident of Cherokee County, Alabama. Hulsey received medical treatment at Riverview Regional Medical Center in Etowah County, Alabama at all times material to this Complaint.

9. Defendant Community Health Systems, Inc. ("CHS") is a Delaware corporation with its principal place of business in Tennessee. Upon information and belief, CHS does business in 29 states, including Alabama. CHS is the parent company that owns and operates, through subsidiaries, 206 general acute care hospitals in 29 states with approximately 31,000 licensed beds. CHS is, or was at all relevant times, the parent company of Gadsden Regional Medical Center and Riverview Regional Medical Center.

10. Defendant Community Health Systems Professional Services Corporation (hereinafter "CHSPSC") is a Delaware corporation with its principal place of business in Tennessee. Upon information and belief, CHSPSC does business in Alabama as well as 28 other states. CHSPSC is also registered to conduct business in Alabama. CHSPSC conducts business throughout this District, Alabama, and the United States.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from Defendants, (b) the amount in controversy exceeds $5,000,000 exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

12. This Court has personal jurisdiction over Defendants because they are registered to conduct business in Alabama, regularly conduct business in Alabama, have hospitals and other offices located in Alabama, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from Alabama.

13. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Defendants do business throughout this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district. Venue is additionally

proper because Defendants maintain hospitals and other administrative offices in this district.

FACTS COMMON TO ALL COUNTS

14. Plaintiffs are patients and customers of Defendants' hospitals.

15. In the regular course of business, Defendants collect and maintain possession, custody, and control of a wide variety of Plaintiffs' Sensitive Information, including, but not limited to patient names, addresses, birthdates, telephone numbers, social security numbers, patient credit card, medical or clinical information and history.

16. Plaintiffs and Defendants agreed that, as part of the services provided to Plaintiffs, Defendants would protect Plaintiffs' Sensitive Information.

17. Through its Notice of Privacy Practices (which all patients receive upon admission to Defendants hospitals and facilities), Community Health represented that it would protect its patients' Sensitive Information and keep it confidential.

18. Community Health reiterated its obligations to protect its patients' Sensitive Information through many of its affiliate hospitals' "Patient Rights and Responsibilities" agreements, which stated that patients had the right to have their medical records to be treated as private.

19. The agreements to protect Plaintiffs' Sensitive Information were a value added to the services provided by Defendants that was considered a benefit of the bargain for which Plaintiffs paid adequate consideration.

20. Upon information and belief, a portion of the consideration paid by Plaintiffs was accepted and rendered proceeds by Defendants that was allocated to protecting and securing Sensitive Information and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and customers, such as Plaintiffs, to add value to the services provided by agreeing to protect Sensitive Information.

21. Defendants stored Plaintiffs' Sensitive Information in an unprotected, unguarded, unsecured, and/or otherwise unreasonably protected electronic and/or physical location.

22. Defendants did not adequately encrypt, if at all, Plaintiffs' Sensitive Information.

23. Defendants did not provide adequate security measures to protect Plaintiffs' Sensitive information.

24. On or about August 18, 2014, Community Health filed a Form 8-K with the United States Securities and Exchange Commission that provided the first notification of the data breaches. This filing stated that Community Health's computer network was the target of an "external, criminal cyber-attack that [it]

believes occurred in April and June, 2014 and the data breach "affected approximately 4.5 million individuals" This filing also states that those who are affected were provided services by Community Health within the last five years.

25. Defendants' failure to notify its patients of this data breach in a reasonable time caused Plaintiffs to remain ignorant of the breach and, therefore, Plaintiffs were unable to take action to protect themselves from harm.

26. Defendants designed and implemented their policies and procedures regarding the security of protected health information and Sensitive Information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected health information and other Sensitive Information. Upon information and belief, Defendants failed to encrypt, or adequately encrypt, Plaintiffs' Sensitive Information.

27. By failing to fulfill their promise to protect Plaintiffs' Sensitive Information, Defendants have deprived Plaintiffs' of the benefit of the bargain. As a result, Defendants cannot equitably retain payment from Plaintiffs—part of which was intended to pay for the administrative costs of data security—because Defendants did not properly secure Plaintiffs' information and data.

28. Community Health's statements about its data security and management practices-both through its privacy policies and public representations-

served to falsely inflate the advertised utility of its services, thus allowing it and/or its affiliates to charge patients higher costs for treatment.

29. Community Health's data breach resulted from a variety of failures to follow HIPAA guidelines and industry standards. Among such deficient practices, Community Health's breach shows that it failed to implement, or inadequately implemented, information security policies or procedures such as those requiring adequate encryption or similar protection of Sensitive Information. For instance, Community Health didn't implement adequate security protections designed to detect and remove security threats, such as malware used to gain access to its servers.

30. Had Community Health implemented proper security protocols to properly encrypt and otherwise protect its patients' Sensitive Information, the consequences of the data breach would have been avoided (as it would have been nearly infeasible to extract its patients' data). Community Health knew or should have known that a security breach could result from its deficient security and privacy practices, as HIPAA and industry standard protections exist specifically to prevent unauthorized access to Sensitive Information and because fixes to the malware that infected its server were readily available.

31. Even though Community Health patients both expected and paid for the above-described security measures as part of their hospital experience (i.e., that

HIPAA-mandated and industry standards would have been used to protect their Sensitive Information), they were not implemented, which resulted in the unsecured release of their Sensitive Information and the loss of paid-for data protection services.

INDIVIDUAL FACTS

PATRICIA MCNUTT

32. McNutt was a patient at Gadsden Regional Medical Center in or around April, May and June of 2013. McNutt provided personal and Sensitive Information to Community Health.

33. As an essential part of the services provided, Community Health agreed to protect her personal and Sensitive Information.

34. As a result of the data breach, McNutt has suffered emotional distress and economic harm, including but not limited to: loss of payment to Defendants—part of which was intended to pay for the administrative costs of data security—because Defendants did not properly secure McNutt's Sensitive Information, diminution in the value of services provided, and future expenses for credit monitoring.

SCOTT HULSEY

35. Hulsey was a patient at Riverview Regional Medical Center in or around December 2013. Hulsey provided personal and Sensitive Information to Community Health.

36. As an essential part of the services provided, Community Health agreed to protect his personal and Sensitive Information.

37. As a result of the data breach, Hulsey has suffered emotional distress and economic harm, including but not limited to: loss of payment to Defendants—part of which was intended to pay for the administrative costs of data security—because Defendants did not properly secure Hulsey's Sensitive Information, diminution in the value of services provided, and future expenses for credit monitoring.

CLASS ACTION ALLEGATIONS

38. Plaintiffs bring this action on behalf of themselves and on behalf of a class of plaintiffs. Plaintiffs bring this action seeking damages on behalf of a class pursuant to the provisions of Rule 23(b)(1), (2), and (3) of the Federal Rules of Civil Procedure on behalf of themselves and a class and subclass of similarly situated individuals defined as:

> **Class:** All persons in the United States and its territories who (i) paid money to Community Health in exchange for health care related services, and (ii) whose Sensitive Information was compromised as a result of the data breach confirmed by Community Health in or around April and June 2014.

Alabama Subclass: All Class members who are residents of the Alabama.

Excluded from the Class and Alabama Subclass (collectively referred to as the "Class," unless otherwise indicated) is (i) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest and their current or former employees, officers and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of Community Health's patient records.

39. **Numerosity**: The exact number of Class members is unknown to Plaintiffs at this time, but on information and belief, the Class is comprised of at least hundreds of thousands of individuals throughout the country, making joinder of each individual member impracticable. Ultimately, the members of the Class will be easily identified through Defendants' records.

40. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members, and include, but are not limited to:

a. Whether Defendants took steps and measures to adequately safeguard Plaintiffs and the Class members' Sensitive Information;

b. Whether Defendants storing of Plaintiffs and the Class members' Sensitive Information in the manner alleged violated industry standards and/or HIPAA;

c. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiff and the members of the Class on the other;

d. Whether Defendants' conduct described herein constitutes a breach of their contracts with Plaintiff and the Class members; and

e. Whether Defendants should retain the monies paid by Plaintiff and other Class members to protect their Sensitive Information.

41. **Typicality:** Plaintiffs claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendants' uniform wrongful conduct during transactions with Plaintiff and the Class.

42. **Adequate Representation:** Plaintiffs will fairly and adequately represent and protect the interests of the Class, and have retained competent and experienced counsel. Plaintiffs have no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiffs.

43. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendants have acted or refused to act on

grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply and affect members of the Class uniformly and Plaintiffs challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs or any other Class member.

44. **Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single

court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

45. Plaintiffs reserve the right to revise Class definitions and questions based upon facts learned in discovery.

COUNT ONE
UNJUST ENRICHMENT

46. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

47. Community Health received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.

48. Community Health did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.

49. Community Health has knowledge of said benefit.

50. Community Health has been unjustly enriched and it would be inequitable for Defendants' to retain Plaintiffs' payments.

51. As a result, Plaintiffs have been proximately harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT TWO
BREACH OF EXPRESS CONTRACT

52. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

53. Plaintiffs and the Class members' paid money to Community Health in exchange for its promise to provide patient services.

54. In addition to providing medical care, a material part of Community Health's promise to provide patient services involved protecting Plaintiffs and the Class members' Sensitive Information.

55. In its written agreements as well as its patients' rights and privacy notices, Community Health expressly promised Plaintiffs and members of the Class that Community Health only discloses health information when required to do so by federal or state law. Community Health further promised that it would protect their Sensitive Information.

56. Community Health promised to comply with all HIPAA standards and to make sure that Plaintiffs and the Class members' Sensitive Information was protected. Community Health further promised to provide notice to Plaintiffs and members of the Class describing Community Health's legal duties and privacy practices with respect to their Sensitive Information.

57. The contracts required Community Health to safeguard Plaintiffs and the Class members' Sensitive Information to prevent its disclosure and/or unauthorized access

58. Plaintiffs and the Class members fully performed their obligations under the contracts.

59. Community Health did not adequately safeguard Plaintiffs and the Class members' protected Sensitive Information. Specifically, Community Health did not comply with its promise to comply with HIPAA's guidelines or industry standards when it stored its patients' Sensitive Information.

60. The failure to meet these promises and obligations constitutes an express breach of contract. In other words, Community Health breached the contracts with Plaintiffs and the members of the Class by failing to implement sufficient security measures to protect Plaintiffs and the Class members' Sensitive Information.

61. Community Health's failure to fulfill its data security and management promises resulted in Plaintiffs and the Class members receiving services that were of less value than they paid for (i.e., the provision of medical care without adequate data security and management practices).

62. Stated otherwise, because Plaintiffs and the Class paid for privacy protections that they did not receive-even though such protections were a material

part of their contracts with Community Health-Plaintiffs and the Class did not receive the full benefit of their bargain.

63. As a result of Community Health's breach, Plaintiffs and the Class suffered damages in the amount of the difference between the price they paid for Community Health's services as promised and the actual diminished value of its health care services.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and other damages as may be provided by law, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT THREE
BREACH OF IMPLIED CONTRACT

64. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

65. In order to benefit from Community Health's services, Plaintiffs and the Class disclosed Sensitive Information to Community Health, including their names, addresses, telephone numbers, Social Security numbers, dates of birth, and extremely sensitive medical diagnosis information.

66. By providing that Sensitive Information, and upon Community Health's acceptance of such information, Plaintiffs and the Class, on the one hand,

and Community Health, on the other hand, entered into implied contracts whereby Community Health was obligated to take reasonable steps to secure and safeguard that information.

67. Under the implied contract, Community Health was further obligated to provide Plaintiffs and the Class with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

68. Without such implied contracts, Plaintiffs and the Class would not have provided their personal information to Community Health.

69. As described herein, Community Health did not take reasonable steps to safeguard Plaintiffs' and the Class members' Sensitive Information.

70. Because Community Health allowed unauthorized access to Plaintiffs' and the Class members' Sensitive Information and failed to take reasonable steps to safeguard their Sensitive Information, Community Health breached its implied contracts with Plaintiffs and the Class.

71. The failure to meet these promises and obligations constitutes a breach of contract. In other words, Community Health breached the contracts by failing to implement sufficient security measures to protect Plaintiffs and the Class members' Sensitive Information as described herein.

72. Community Health's failure to fulfill its data security and management promises resulted in Plaintiff and the Class receiving services that were of less

value than they paid for (i.e., the provision of medical care without adequate data security and management practices).

73. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive-even though such protections were a material part of their contracts with Community Health-Plaintiff and the Class did not receive the full benefit of their bargain.

74. As a result of Community Health's breach, Plaintiffs and the Class suffered damages in the amount of the difference between the price they paid for Community Health's services as promised and the actual diminished value of its health care services.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and other damages as may be provided by law, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT FOUR
NEGLIGENCE AND WANTONNESS

75. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

76. Defendants requested and came into possession of Plaintiffs' Sensitive Information and had a duty to exercise reasonable care in safeguarding

and protecting such information from being accessed. Defendants' duty arose, *inter alia*, from the industry standards and its relationship with Plaintiffs.

77. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' Sensitive Information. The breach of security, unauthorized access, and resulting injury to Plaintiffs' and the Class were reasonably foreseeable, particularly in light of Defendants' inadequate data security system and failure to adequately encrypt the data.

78. Defendants, through their negligent and wanton actions or omissions, unlawfully breached their duty to Plaintiffs by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiffs' Sensitive Information within Defendants' control.

79. Defendants, through their negligent and wanton actions and/or omissions, breached their duty to Plaintiffs by failing to have procedures in place to detect and prevent access to Plaintiffs' Sensitive Information by unauthorized persons.

80. But for Defendants' breach of its duties, Plaintiffs' Sensitive Information would not have been compromised.

81. Plaintiffs' Sensitive Information was stolen and accessed as the proximate result of Defendants failing to exercise reasonable care in safeguarding

such information by adopting, implementing, and maintaining appropriate security measures and encryption.

82. As a result, Plaintiffs have been harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT FIVE
NEGLIGENCE PER SE

83. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

84. Defendants' violation of HIPAA resulted in an injury to Plaintiffs.

85. Plaintiffs fall within the class of persons HIPAA was intended to protect.

86. The harm Defendants caused Plaintiffs are injuries that result from the type of behavior that HIPAA was intended to protect.

87. As a result, Plaintiffs have been harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by

a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT SIX
MONEY HAD AND RECEIVED

88. Plaintiffs repeat and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

89. Defendants have received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.

90. Defendants did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.

91. The law creates an implied promise by Defendants to pay it to Plaintiffs.

92. Defendants have breached said implied promise.

93. Defendants breach has proximately caused Plaintiffs to suffer harm and damages.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above

described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

RELIEF REQUESTED

WHEREFORE, Plaintiffs request that this Court:

a. Determine that this action may be maintained as a class action under Fed. R. Civ. P. 23;

b. Find that Defendants are liable under all legal claims asserted herein for their failure to safeguard Plaintiffs' and Class members' Sensitive Information;

c. Award injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Defendants to protect all data collected through the course of its business in accordance with HIPAA and industry standards, (iii) consumer credit protection and monitoring services for Plaintiffs; and (iv) consumer credit insurance to provide coverage for unauthorized use of Plaintiffs' personal information, medical information, and financial information;

d. Award damages, including statutory damages where applicable and punitive damages, to Plaintiffs and the Classes in an amount to be determined at trial;

e. Award restitution for any identity theft, including, but not limited to payment of any other costs, including attorneys' fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of Defendants' actions;

f. Award restitution in an amount to be determined by an accounting of the difference between the price Plaintiffs and the Classes paid in reliance upon Defendants' duty/promise to secure its members' Sensitive Information, and the actual services—devoid of proper protection mechanisms—rendered by Defendants;

g. Award costs and attorneys' fees to Plaintiffs; and

h. Award any such other and further relief as may be just and proper.

This the 5th day of February, 2015.

Respectfully submitted,

/s/ Wm. Eric Colley
WM. ERIC COLLEY
AL State Bar No. ASB-0450-L56W
P.O. Box 681045
Fort Payne, AL 35968
Telephone: 256-845-8101
Email: colleyw@bellsouth.net

/s/ J. Michael Bowling
J. Michael Bowling
AL State Bar No. ASB-8261-W86J
Email: mbowling@friedman-lawyers.com
Christopher J. Zulanas
AL State Bar No. ASB-1572-U82C
Email: czulanas@friedman-lawyers.com
3800 Corporate Wood Drive
Birmingham, AL 35242
Attorneys for Plaintiffs and the Proposed Class

JURY DEMAND

Plaintiffs demand a trial by jury.

/s/ Wm. Eric Colley
Of Counsel

REQUEST FOR SERVICE

Pursuant to FRCP 4.1 and 4.2, Plaintiffs request service of the foregoing Complaint by certified mail.

/s/ Wm. Eric Colley
Of Counsel

PLEASE SERVE DEFENDANTS BY CERTIFIED MAIL AS FOLLOWS:

Community Health Systems, Inc.
Corporation Service Company
2711 Centerville Road
Suite 400
Wilmington, DE 19808

Community Health Systems Professional Services Corporation
CSC-Lawyers Incorporating Svc Inc.
150 South Perry Street
Montgomery, AL 36104